STRATEGY
RESEARCH
PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

PROTECTING AMERICA'S CRITICAL INFRASTRUCTURE

BY

LIEUTENANT COLONEL WALTER H. FREDERICK, III
United States Army National Guard

USAWC CLASS OF 2002

Prudens Futuri

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

PROTECTING AMERICA'S CRITICAL INFRASTRUCTURE

by

LTC Walter H. Frederick, III
Kansas Army National Guard

COL Ralph D. Ghent, USA
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: LTC Walter H. Frederick, III

TITLE: Protecting America's Critical Infrastructure

FORMAT: Strategy Research Project

DATE: 1 March 2002 PAGES: 36 CLASSIFICATION: Unclassified

Presidential Decision Directive (PDD) 63 was America's first strategy for protecting critical information infrastructures. It has been supplemented with other executive orders and directives. After three years of service PDD 63 has not worked as intended. In this Strategy Research Project I will outline the elements of critical infrastructures, the different policies and problems and challenges of PDD 63. From that I will offer different solutions for critical infrastructure protection.

TABLE OF CONTENTS

LIST OF TABLES

PROTECTING AMERICA'S CRITICAL INFRASTRUCTURE

Presidential Decision Directive (PDD) 63 published in May 1998 was America's first strategy for protecting critical information infrastructures. It has been supplemented with other executive orders and directives. After three years of service PDD 63 has not worked as intended. In this Strategy Research Project I will outline the elements of critical infrastructures, the different policies, problems and challenges of PDD 63 and why America's critical infrastructure and the information systems that manage them are vital national interests. From that I will offer different solutions for critical infrastructure protection.

In PDD 63 President Clinton stated that "critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private."[1] To further define a critical infrastructure, in 1997 the President's Commission on Critical Infrastructure Protection (PCCIP) stated that it is "a network of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services."[2]

In March 1999 former Deputy Secretary of Defense John Hamre claimed "...the United States was in a cyberwar -- under attack by hackers."[3] That was just three years ago. However, the attacks are not just from hackers, they can also be state sponsored or from terrorist organizations. America's critical infrastructure is under attack daily. The following are recent examples that support his comments:

> The National Information Protection Center (NIPC) at the FBI had earlier warned that Chinese hackers would attack U.S.-based Web sites in a campaign to avenge the U.S. spy plane incident and arms sales to Taiwan. Web sites run by the Department of Labor, Health and Human Services and the White House Historical Society were among many defaced with Chinese flags and slogans such as "Beat down imperialism of America!" from groups claiming names such as the "Honker Union of China" and "China Eagle."[4]

These Chinese attacks illustrate that individuals and groups will exploit vulnerabilities in web servers to advance their political agenda and conduct propaganda operations against the United States. Although the damage done can be just a minor annoyance, network administrators have no choice but to remove the compromised web server from service, thereby denying and disrupting its use. The attacked server must be investigated, inspected and cleaned before it can be returned to service. Attacks such as these are against the American political instrument of power. United States Attorney John Gordon in a statement said that:

> A Russian computer programmer imprisoned in the U.S. on charges that he perpetrated a cyber crime spree of extortion and credit card fraud was indicted in California Wednesday - adding the Golden State to a growing list of destinations on the accused hacker's whirlwind tour of American detention centers. Alexey V. Ivanov, 20, was slammed with fifteen counts of computer fraud and extortion for the Southern California portion of a string of financially-motivated attacks on e-commerce companies and small financial institutions, aimed at stealing credit card numbers and consumer information, and strong-arming companies into paying protection money. The federal indictment charges that Ivanov cracked San Diego-based CTS Network Services, and then used the ISP's system to attack other sites. Other victims named in the indictment are Nara Bank in Los Angeles, TransMark Corporation in Rancho Cucamonga, California, and Maryland-based E-Money, an online credit card processing company. "Given the importance of computers in everyday life, hackers and cyber-extortionists pose one of the most significant challenges to law enforcement."[5]

The Russian programmer attacked the financial service sector, one of the eight information systems designated as critical infrastructure. Attacks like this can reduce consumer confidence and trust in the banking industry. These attacks are on the American economic instrument of power.

> A series of sophisticated attempts to break into Pentagon computers has continued for more than three years, and an extensive investigation has produced "disturbingly few clues" about who is responsible, according to a member of the National Security Agency's advisory board. The NSA consultant, James Adams, says U.S. diplomats lodged a formal protest with the Russian government last year after investigators determined that the cyber attacks, which they code-named "Moonlight Maze," appear to have originated from seven Russian Internet addresses. But Russian officials replied that the telephone numbers associated with the sites were inactive and denied any prior knowledge of the attacks, according to Adams. Meanwhile, the assault has continued unabated," Adams wrote in this month's Foreign Affairs magazine, published by the Council on Foreign Relations. "The hackers have built 'back doors' through which they can re-enter the infiltrated systems at will and steal further data; they have also left behind tools that reroute specific network traffic through Russia.[6]

The Moonlight Maze attacks undermine the ability of the Defense Department to conduct operations with the confidence that information and data will remain in the hands of American military personnel. These types of attacks are on the American military instrument of power.

On 11 September 2001, America witnessed a physical attack on its critical infrastructure. The twin towers of the World Trade Center were destroyed with the loss of nearly three thousand Americans after terrorists flew commercial airliners into the buildings. Shortly after that attack the Defense Department's Pentagon suffered a similar attack. It was presumed that another airliner would attack the White House.

As a second order effect of the 11 September attacks, three of the four instruments of America's national power were severely affected. The instruments of power that were damaged were economic, military, and political. The New York Stock Exchange was shut down for ten days, the longest since World War II.[7] Several large financial corporations were either completely destroyed or severely disabled. "Verizon's switching office at 140 West St. in Manhattan, supporting 3.5 million circuits, sustained heavy damage. Verizon Wireless lost 10 cellular transmitter sites,"[8] disrupting cellular communications in New York. "AT&T lost fiber optic equipment in the World Trade Center and had switching equipment damaged in a nearby building. Remarkably, AT&T switching gear in the basement of the World Trade Center continued to function."[9]

After the attack in Washington D.C., the Pentagon was evacuated for several hours and is still being rebuilt. Many Defense Department servers and computers were destroyed. Several information management systems were destroyed in the attack on the Pentagon and vital communications were disrupted. As a precaution the White House and the United States Capitol were evacuated.

After the second airliner hit the World Trade Center, the Federal Aviation Administration (FAA) grounded all air traffic in the United States and inbound international traffic. The air transportation industry was effectively shut down for at least a day. This was the first time in history this had ever occurred. The grounding order lasted for over 24 hours. General aviation would be grounded for several more days. Ronald Reagan National Airport, a vital transportation hub for Washington, D.C. would be closed for nearly a month. This move by the FAA caused several air carriers to lay off thousands of workers causing bankruptcy worries.[10] The aviation sector of America's critical transportation infrastructure was grounded.

From viewing the different examples above, America's critical infrastructure has been attacked in many different ways with varying degrees of disruption, destruction, theft or denial of service. The critical infrastructure must be improved to sustain America's economy and global power. In the next section I will discuss the policies of the Clinton and George W. Bush administrations for critical infrastructure protection.

CRITICAL INFRASTRUCTURE PROTECTION – A VITAL NATIONAL INTEREST

The Clinton and Bush administrations have declared that America's critical infrastructure is a vital national interest. President Clinton's National Security Strategy for a Global Age published in December 2000 affirms that with the following statement: "Vital interests are those directly connected to the survival, safety and vitality of our nation. Among these are…protection of our critical infrastructures -- including energy, banking and finance, telecommunications, transportation, water systems, vital human services, and government operations."[11] President Clinton published Executive Order 13010 - Critical Infrastructure Protection, in July 1996. In the document President Clinton states, "Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[12]

President George W. Bush recognized the importance of "ensuring the continued operation of America's critical information services."[13] He stated in his 2002 state of the union address, "we'll protect our homeland."[14] His demonstration of support has been through Executive Order 13231 - Critical Infrastructure Protection in an Information Age, published in October 2001. This document complements previous Clinton administration policies. In testimony to Congress, Bush appointee John S. Tritak, the Director of the Critical Infrastructure Assurance Office (CIAO), stated: "As vital as our nation's critical infrastructures are to the American way of life, the authority to protect those infrastructures must be a priority; and the resources must match the rhetoric."[15] The United States Department of State Strategic Plan states that [it is the strategy of the State Department to] reduce the likelihood of and vulnerability to attacks on critical infrastructure, including information systems, by developing global solutions, norms, and agreements. Promote an international framework for tracking and managing cyber attacks."[16]

In a speech on 22 March 2001 at the meeting of the United States Chamber of Commerce's Partnership for Critical Infrastructure, Condoleezza Rice, the Assistant to the President on National Security Affairs stated that "...critical infrastructure protection is a critically important issue -- one that is squarely on our radar screen at the National Security Council. The President himself is on record as stating that infrastructure protection is important to [our] economy and national security, and it will be a priority for my Administration."[17]

So, there are numerous indications from both the Clinton and Bush Administrations that critical infrastructure protection is a vital national interest. Both administrations have published several directives to deal with the problem of critical infrastructure protection.

President Clinton appointed the President's Commission on Critical Infrastructure Protection also known as the PCCIP in 1996. The PCCIP determined that the telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply system, emergency service (including medical, police, fire, and rescue), and continuity of government were vital to America's security and must be protected.[18]

President Clinton's Executive Order 13010 required the Commission on Critical Infrastructure Protection have an interagency membership from several departments and agencies. The commission was to terminate after one year. Those agencies involved were the Departments of Treasury, Justice, Defense, Commerce, Transportation, Energy and the Central Intelligence Agency, Federal Emergency Management Agency, Federal Bureau of Investigation and the National Security Agency. Each of these interagency commission members have two full-time members on the commission. The executive order authorized a steering committee for the PCCIP. The committee has four members appointed by the President. One of the appointees must be the Chairman, and another an employee of the Executive Office of the President (EOP). The commission's job is six-fold: consult with owners of critical infrastructure in the public and private sector; assess the scope and nature of America's critical infrastructures vulnerabilities, determine legal and policy issues; recommend national policy and strategy; propose new public and administrative laws; and provide reports and recommendations to the steering committee.

PRESIDENTIAL DECISION DIRECTIVE 63

From the PCCIP President Clinton published Presidential Decision Directive 63 (PDD 63) on 22 May 1998. PDD 63 is the seminal document from which critical infrastructure protection has developed. In PDD 63 President Clinton states, "It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. I intend that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."[19] With that he had several national goals that were to be accomplished by the year 2000. Those goals were:

> The United States shall have achieved an initial operating capability and no later than five years from today the United States shall have achieved and shall maintain the ability to protect the nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:
>
> - The Federal Government to perform essential national security missions and to ensure the general public health and safety;
> - State and local governments to maintain order and to deliver minimum essential public services;
> - The private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services;

- Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States.[20]

With PDD 63 the Clinton administration added some critical infrastructure structure to the federal government. Because there was a lack of structure prior to PDD 63 there were four organizations developed. They were Lead Agencies for Sector Liaison, Special Functions, Interagency Coordination, and the National Infrastructure Assurance Council.

The Lead Agencies for Sector Liaison were developed for each infrastructure sector that could be a target for significant cyber or physical attack.[21] This allowed for a single federal agency or department point of contact. For instance, the Department of Energy is the single point of contact for all critical infrastructure protection of electrical power, oil and gas production and storage in America. The Lead Agencies for Sector Liaison would also be the point of contact at the National Infrastructure Protection Center. The actual person who is the point of contact official must be at the secretary rank or higher.[22] Together, the Lead Agency and the private sector counterparts will develop and implement a Vulnerability Awareness and Education Program for their sector.[23]

The Federal government performs Lead Agencies for Special Functions. They are comprised of national defense, foreign affairs, intelligence, and law enforcement.[24] Each lead agency is required to appoint a senior officer of Assistant Secretary rank or higher to serve as the Functional Coordinator for that function for the Federal Government.[25]

The Sector Liaison Officials and Functional Coordinators of the Lead Agencies, as well as representatives from other relevant departments and agencies, including the National Economic Council, will meet to coordinate the implementation of this directive under the auspices of a Critical Infrastructure Coordination Group (CICG), chaired by the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism.[26] The National Coordinator works for the Assistant to the President for National Security Affairs and is appointed by the President.[27] The National Coordinator assures appropriate coordination with the Assistant to the President for Economic Affairs.[28]

The fourth body organized was the National Infrastructure Assurance Council. A presidential appointee chairs the council.[29] The President appoints a panel of major infrastructure providers and state and local government officials to serve on the National Infrastructure Assurance Council.[30] The Council is required to meet periodically to enhance the partnership of the public and private sectors in protecting critical infrastructures.[31] Senior

Federal Government officials are required to participate in the meetings of the National Infrastructure Assurance Council when necessary.[32]

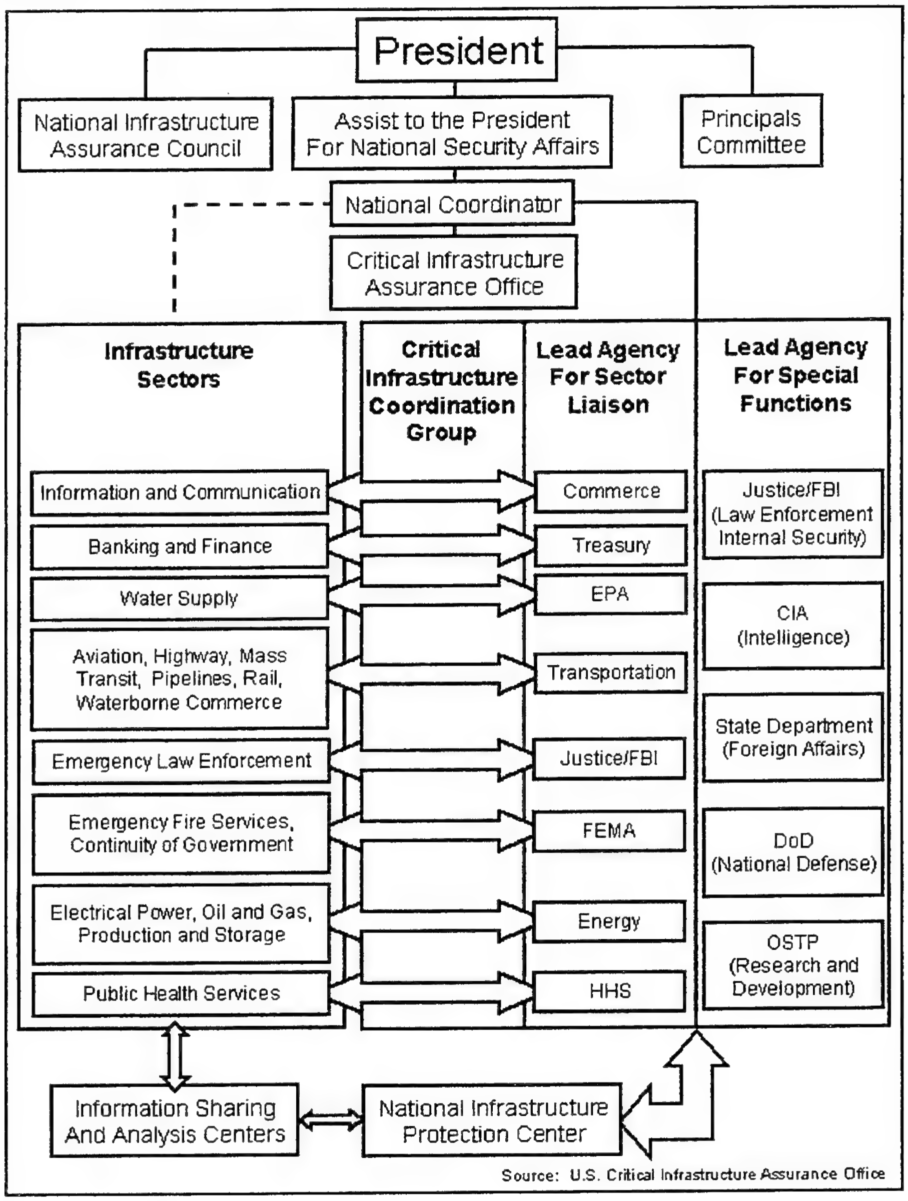
Our National Infrastructure is mostly owned and operated by the private sector.[33] President Clinton recognized that in PDD 63 and wanted a public – private partnership to solve the challenges of critical infrastructure protection. PDD 63 establishes some structure to deal with critical infrastructure protection. For each sector of the economy that is designated as critical, PDD 63 assigned a lead agency for public – private coordination. It was broken out in the following table:

Critical Infrastructure	Lead Federal Agency
Information and Communications	Department of Commerce
Banking and Finance	Department of Treasury
Water Supply	Environmental Protection Agency
Aviation, Highways, Mass Transit, Pipelines, Rail, Waterborne Commerce	Department of Transportation
Emergency Law Enforcement	Department of Justice and Federal Bureau of Investigation
Emergency Fire Services and Continuity of Government	Federal Emergency Management Agency
Electrical power, oil and gas production and storage	Department of Energy
Public Health Service	Health and Human Services
Special Functions	
Law enforcement and internal security	Department of Justice and the Federal Bureau of Investigation
Foreign intelligence	Central Intelligence Agency
Foreign affairs	Department of State
National defense	Department of Defense

TABLE 1 PUBLIC – PRIVATE SECTOR RELATIONSHIPS

Presidential Decision Directive 63 also authorizes two organizations in the federal government for warning and information sharing. The centers were the National Infrastructure Protection Center (NIPC) and the Information Sharing and Analysis Center (ISAC).[34]

The NIPC is organized under the control of the Federal Bureau of Investigation. The NIPC will provide a national focal point for gathering information on threats to the infrastructures.[35] It has Federal Bureau of Investigation, United States Secret Service and other investigators experienced in computer crimes and infrastructure protection, as well as representatives detailed from the Department of Defense, the Intelligence Community and Lead Agencies. It is linked electronically to the rest of the Federal Government, including other warning and operations centers, as well as any private sector sharing and analysis centers. Its mission includes providing timely warnings of international threats, comprehensive analysis and law enforcement investigation and response.[36] The relationship between the President, the Assistant to the President for National Security Affairs, the National Coordinator and other actors for Critical Infrastructure Protection is illustrated below:


President
National Infrastructure Assurance Council
Assist to the President For National Security Affairs
Principals Committee
National Coordinator
Critical Infrastructure Assurance Office
Infrastructure Sectors
Critical Infrastructure Coordination Group
Lead Agency For Sector Liaison
Lead Agency For Special Functions
Information and Communication
Banking and Finance
Water Supply
Aviation, Highway, Mass Transit, Pipelines, Rail, Waterborne Commerce
Emergency Law Enforcement
Emergency Fire Services, Continuity of Government
Electrical Power, Oil and Gas, Production and Storage
Public Health Services
Commerce
Treasury
EPA
Transportation
Justice/FBI
FEMA
Energy
HHS
Justice/FBI (Law Enforcement Internal Security)
CIA (Intelligence)
State Department (Foreign Affairs)
DoD (National Defense)
OSTP (Research and Development)
Information Sharing And Analysis Centers
National Infrastructure Protection Center

Source: U.S. Critical Infrastructure Assurance Office

TABLE 2 CRITICAL INFRASTRUCTURE PROTECTION RELATIONSHIPS

The ISAC is how an industry sector coordinates information sharing among members and between the sector and the NIPC. The National Coordinator, working with Sector Coordinators, Sector Liaison Officials and the National Economic Council, consults with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center.[37] According to the System Administration, Networking, and Security (SANS) Institute a cooperative research and education organization, there are two models for ISACs.[38] This is because what works for one part of the critical infrastructure may not work for another.

The first model is for the private sector. It is called the Financial Services ISAC (FS/ISAC).[39] The financial services industry was the first to form an ISAC. The main focus of this ISAC is only focused on cyber threats. It was formed as a limited liability corporation (LLC) and is open to banks that are members of the Federal Deposit Insurance Corporation (FDIC). For their protection, the members of the ISAC are kept confidential.

The FS/ISAC is a secure database that provides for authenticated and anonymous sharing of information associated with threats, incidents, and vulnerabilities of industry assets and available resolutions or solutions. The FS/ISAC is Internet based, allowing authorized participants to securely share information with other authorized members of the financial services industry.[40]

There is utility in the secrecy in the first model. When a bank suffers the loss from an Internet based theft, the bank is not likely to want to share that information with their stockholders, customers, FDIC, Treasure Department or other banks. Because the vulnerability that exists at one bank could exist at another. This information must be shared. The best way to share is with this model of confidentiality. If a private sector organization won't share the lessons learned from a loss, the system has failed.

The second model recommended by SANS is the National Coordinating Center for Telecommunications ISAC (NCC-ISAC) and is just two years old. With this model there is no confidentiality, and it is focused on all threats, including cyber. Industry membership in the NCC is open to "all U.S. telecommunications industry entities that provide domestic or international communications services; local or long-haul communications services; voice or data (including software) communications services; or telecommunications equipment supply services."[41]

There are legal problems with this type of public-private ISAC. Because of Freedom of Information Act (FOIA) requirements, which provide the public access to records maintained by the government, there could potentially be a release of private sector data shared with the government participants in the NCC-ISAC.[42]

THE EIGHT AREAS OF CRITICAL INFRASTRUCTURE – A CLOSER LOOK

The following is a closer look at the eight critical infrastructures and how they interact with information networks to function efficiently.

Electrical Power Systems: The generation stations, transmission and distribution networks that create and supply electricity to end-users so that end-users achieve and maintain nominal functionality, including the transportation and storage of fuel essential to that system.[43] The national electric grid relies on Global Positioning System (GPS) to ensure line stability and find disruptions.[44] Of the eight critical infrastructures the electrical power systems have embraced the computer revolution more aggressively than the others.[45]

Gas and Oil Production, Storage and Transportation: The holding facilities for natural gas, crude and refined petroleum, and petroleum-derived fuels, the refining and processing facilities for these fuels and the pipelines, ships, trucks, and rail systems that transport these commodities from their source to systems that are dependent upon gas and oil in one of their useful forms.[46]

Banking and Finance: The retail and commercial organizations, investment institutions, exchange boards, trading houses, and reserve systems, and associated operational organizations, government operations, and support entities, that are involved in all manner of monetary transactions, including its storage for saving purposes, its investment for income purposes, its exchange for payment purposes, and its disbursement in the form of loans and other financial instruments.[47] The financial sector employs GPS timing to synchronize its encrypted computer networks.[48]

Transportation: The aviation, rail, highway, and aquatic vehicles, conduits, and support systems by which people and goods are moved from a point-of-origin to a destination point in order to support and complete matters of commerce, government operations, and personal affairs.[49] The transportation industry relies increasingly on GPS for navigational purposes.[50]

Water Supply Systems: The sources of water, reservoirs and holding facilities, aqueducts and other transport systems, the filtration and cleaning systems, the pipelines, the cooling systems and other delivery mechanisms that provide for domestic and industrial applications, including systems for dealing with waste water and fire fighting.[51]

Emergency Services: The medical, police, fire and rescue systems and personnel that are called upon when an individual or community is responding to a public health or safety incident where speed and efficiency are necessary.

Continuity of Government Services: Those operations and services of governments at federal, state, and local levels critical to the functioning of the nation's systems, i.e., public health, safety, and welfare.[52]

Telecommunications: The networks and systems that support the transmission and exchange of electronic communications among and between end-users (such as networked computers).[53] The telecommunications industry relies on GPS for time and frequency synchronization.[54]

Because there is such a reliance on GPS to manage several critical infrastructures, a report by the Heritage Foundation recommends that it be added as a ninth critical infrastructure. The report states that "[d]isruption by terrorist groups or hostile states could jeopardize America's homeland security, but the GPS has not been designated as a vital national asset."[55]

EXECUTIVE ORDER 13231 – CRITICAL INFRASTRUCTURE PROTECTION IN THE INFORMATION AGE

President Bush also recognizes the importance of critical infrastructure protection. On 18 October 2001, with only ten months in office and even before publishing a National Security Strategy he published Executive Order 13231 - Critical Infrastructure Protection in an Information Age. Executive Order 13231 does not supersede PDD 63. They both establish end-states for critical infrastructure protection, establishing boards and their memberships, as well as interagency and agency responsibilities for critical infrastructure protection.

When President Clinton published PDD 63 and sent it to the primary federal government agencies it had good guidance for critical infrastructure protection. The delineation of what is critical differs between the two directives. Clinton uses the terms banking and financial. President Bush uses the broader term of financial services. President Bush also added manufacturing and health care as part of the critical infrastructure.[56]

It was wise to add manufacturing. The reason for this is there have been so many mergers in the defense industry; there are not as many corporations the Department of Defense can choose from for contracting vital defense equipment. For example, Boeing is the only contractor for cargo aircraft in the country. There were only two competitors for the Joint Strike Fighter, Boeing and Lockheed Martin. America cannot afford to loose, or have disruption in the manufacturing done by Boeing and Lockheed Martin. They are national assets.

PDD 63 discusses the lead agency for critical infrastructure protection. It does not, however, state who the one single lead is for CIP. Bush assigns that task to each agency. For special functions (national defense, foreign affairs, intelligence, law enforcement) it states there should also be lead agencies. President Clinton assigned the lead for the special functions to be an Assistant Secretary or higher.

In Executive Order 13231 President Bush designates the Office of Management and Budget (OMB) as the lead executive agency for protecting Executive Branch Information Systems Security. For National Security Information Systems he appointed the Secretary of Defense and Director, Central Intelligence (DCI) who have the responsibility for their respective departments. This means there are three lead agencies for critical infrastructure protection in the United States. The Assistant to the President for National Security Affairs will advise the President when there is a deficiency in the security practices of a department or agency.

As stated earlier, President Clinton established the National Infrastructure Protection Center for threats, warnings, vulnerabilities and law enforcement investigation and response. There is little mention in President Bush's Executive Order about the NIPC other than working with the CIP Board in a similar fashion as with Clinton's National Coordinator. The CIP Board is a cabinet secretary-level board that will bring about a higher level of interest in information protection. In the board President Bush established there are many responsibilities that complement PDD 63. The board is responsible for outreach to the private sector and state and local governments. It will work with the private sector and state and local governments to share information. It will coordinate incidents and crisis response. It is responsible for recruiting, retaining and training executive branch professionals. It will be the lead for coordination of Research and Development. It will coordinate with Law Enforcement and National Security Components and International Information Infrastructure Protection.

International Information Infrastructure Protection was not mentioned in PDD 63. This problem was addressed in Executive Order 13231. With the globalization of America's economy International Information Infrastructure must be addressed. All global and transnational companies rely on the internet to conduct business with America, consequently this issue must be addressed.

Finally, President Bush's executive order revokes Executive Order 13130. This executive order authorized the National Infrastructure Assurance Council. With President Bush's Executive Order 13231 it is replaced with the National Infrastructure Advisory Council.

THREATS TO AMERICA'S CRITICAL INFRASTRUCTURE

So what are the threats? The PCCIP identified ten potential cyber threats to America's critical infrastructure.

Natural events and accidents. Storm-driven wind and water regularly cause service outages, but the effects are well known, the providers are experienced in dealing with these situations, and the effects are limited in time and geography.

Accidental Physical Damage. Accidental physical damage to facilities is known to cause a large fraction of system incidents. Common examples are fires and floods at central facilities and the ubiquitous backhoe that unintentionally severs pipes or cables.

Blunders, errors, and omissions. By most accounts, incompetent, inquisitive, or unintentional human actions (or omissions) cause a large fraction of the system incidents that are not explained by natural events and accidents. Since these usually only affect local areas, service is quickly restored; but there is potential for a nationally significant event.

Insiders. Normal operation demands that a large number of people have authorized access to the facilities or to the associated information and communications systems. If motivated by a perception of unfair treatment by management, or if suborned by an outsider, an "insider" could use authorized access for unauthorized disruptive purposes.

Recreational hackers. For an unknown number of people, gaining unauthorized electronic access to information and communication systems is a most fascinating and challenging game. Often they deliberately arrange for their activities to be noticed even while hiding their specific identities. While their motivations do not include actual disruption of service, the tools and techniques they perfect among their community are available to those with hostile intent.

Criminal activity. Some are interested in personal financial gain through manipulation of financial or credit accounts or stealing services. In contrast to some hackers, these criminals typically hope their activities will never be noticed, much less attributed to them. Organized crime groups may be interested in direct financial gain, or in covering their activity in other areas.

Industrial espionage. Some firms can find reasons to discover the proprietary activities of their competitors, by open means if possible or by criminal means if necessary. Often these are inter-national activities conducted on a global scale.

Terrorism. A variety of groups around the world would like to influence US policy and are willing to use disruptive tactics if they think that will help.

National intelligence. Most, if not all, nations have at least some interest in discovering what would otherwise be secrets of other nations for a variety of economic, political, or military purposes.

Information warfare. Both physical and cyber attacks on our infrastructures could be part of a broad, orchestrated attempt to disrupt a major US military operation or a significant economic activity.[57]

THE ROLES AND MISSIONS OF THE NATIONAL INFRASTRUCTURE PROTECTION CENTER

The National Infrastructure Protection Center (NIPC) was authorized and established by PDD 63 in May 1998. It is located at the Federal Bureau of Investigation (FBI) building in Washington D.C. The FBI has the responsibility to manage the NIPC. The NIPC's mission is to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against American critical infrastructures.[58]

The NIPC posts warnings on its web site as well as distribution to critical sector coordinators, InfraGard members, and general law enforcement authorities.[59] The NIPC is linked electronically to the rest of the federal government, including other warning and operation centers, as well as private sector Information Sharing and Analysis Centers (ISAC).[60]

As a way to share information the NIPC established a program called InfraGard. At its most basic level, InfraGard is a cooperative undertaking between the U.S. Government led by the FBI and the NIPC and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States critical infrastructures.[61] The National InfraGard Program began as a pilot project in 1996, when the Cleveland FBI Field Office asked local computer professionals to assist the FBI in determining how to better protect critical information systems in the public and private sectors.[62]

Because the NIPC is a part of the FBI there has been some friction. Law enforcement agencies are not normally in the information sharing business, but PDD 63 gave it the often conflicting missions of information sharing and law enforcement.[63] The Heritage Foundation in its report, Defending the American Homeland. A Report of The Heritage Foundation Homeland Security Task Force states:

> "This dual-track mission undermines cooperation with the private sector on information sharing. Though the NIPC's information-sharing mechanisms work rather well, many in the private sector remain cautious in sharing such information as network intrusions with the Center because of its concurrent law enforcement role. Businesses have no way of knowing whether the information they share about network security could be used to build a criminal case against them."[64]

The authors of the report believe the NIPC should be moved from under the FBI's authority and placed under the Department of Commerce. Their rational is because "PDD–63 designated the Commerce Department as lead agency for information technology and the communication industry, and moving the NIPC to Commerce will complement this mission."[65] The Heritage Foundation also believes that "...the Commerce Department has significant experience working with the hi-tech industry and implementing policy, both through the National Telecommunications and Information Agency (NTIA), which administers the department's responsibilities under PDD–63, and the Technology Administration."[66]

THE ROLE OF THE OFFICE FOR HOMELAND SECURITY

There have been many debates as to the role of the Office for Homeland Security established after the 11 September 2001 terrorist attack on America. It is uncertain how this new office will deal with critical infrastructure protection. According to testimony at a hearing in October 2001 at the House Committee on Science about vulnerability of our nation's computer infrastructure, the office will "...coordinate 40 federal agencies and departments and oversee everything from the interaction between the FBI and the CIA in developing and using intelligence to the interaction between governors and state agencies to prepare for potential attacks."[67]

According to the report by the Heritage Foundation the Office for Homeland Security should take a large role in critical infrastructure protection. The report states that the "President should require the Office of Homeland Security to provide annual assessments of Federal efforts on protecting vital infrastructure."[68] The authors of the report also believe that the Office of Homeland Security should "...develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks."[69] The report further recommends "...the Sector Liaison Officials report as soon as possible, and thereafter annually, to the Director of Office of Homeland Security on the status of security for infrastructure under their jurisdiction." [70] If this recommendation becomes policy, the Office of Homeland Security will have a broad role in critical infrastructure protection.

RESPONSIBILITIES OF THE DEFENSE DEPARTMENT

The Defense Department has numerous responsibilities for critical infrastructure Protection. When President Bush issued Executive Order 13231 for Critical Infrastructure Protection in the Information Age he designated the Secretary of Defense as executive agent for the protection of National Security Information Systems, except those under the umbrella of the Director of Central Intelligence (DCI).

The Secretary of Defense has responsibility to oversee, develop, and ensure implementation of policies, principles, standards, and guidelines for the security of information systems that support defense operations. The Secretary of Defense must coordinate the development of policies, principles, standards, and guidelines for the security of national security information systems that support the operations of other executive branch departments and agencies with national security information with the Assistant to the President for National Security Affairs (APNSA).

Executive Order 13231 establishes the President's Critical Infrastructure Protection Board (CIPB). The Secretary of Defense and Chairman, Joint Chief of Staff each have a position on the CIPB in accordance with Executive Order 13231. The CIPB has several standing committees. The Defense Department has responsibility in two of them. One is the Committee on National Security Systems and is a re-designation of The National Security Telecommunications and Information Systems Security Committee, established by NSD-42. It is chaired by the Department of Defense. The Defense Department is the co-chair for the Incident Response Coordination Committee sharing it with the Attorney General.

Executive Order 13231 requires the Defense Department to submit funding requests to the Office of Management and Budget for demonstration projects and research to support the Board's activities. The Defense Department is still responsible to fund the National Infrastructure Advisor Council (NIAC).

On 30 December 1998 the Defense Department stood up the DoD Joint Task Force - Computer Network Operations (JTF-CNO). JTF-CNO is considered an equivalent to the NIPC that is run by the Federal Bureau of Investigation. Its mission is to work with the Defense Department's unified commands, the services and Department of Defense agencies to defend DoD networks and systems from intruders and other attacks. JTF-CNO and NIPC will share technical information with each other. JTF-CNO is located at the Defense Information Systems Agency (DISA) in Arlington, Virginia. This allows the JTF-CNO to share the existing Intrusion Detection System (IDS) capability of Defense Information Systems Agency (DISA).

THE CHIEF INFORMATION OFFICER IN THE WAR FIGHT

In the federal government Chief Information Officers (CIO) are required for each agency in accordance with federal law. The CIO has numerous duties. Among those is information assurance. Information Assurance is defined as "Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."[71] In accordance with PDD 63:

> "Every department and agency of the Federal Government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems.

> Every department and agency Chief Information Officer (CIO) shall be responsible for information assurance."[72]

PDD 63 also requires that:

> Every department and agency shall appoint a Chief Infrastructure Assurance Officer (CIAO) who shall be responsible for the protection of all of the other aspects of that department's critical infrastructure. The CIO may be double-hatted as the CIAO at the discretion of the individual department. These officials shall establish procedures for obtaining expedient and valid authorizations to allow vulnerability assessments to be performed on government computer and physical systems.

The government Chief Information Officer should plan and budget for Information Assurance training at the user and systems administrator level. The training will raise awareness at the user level and help systems administrators understand vulnerabilities and threats, enabling them to protect critical infrastructure from attack.

Based on the information above the Chief Information Officer is an important part of the war fight as it pertains to the availability, integrity, authentication, confidentiality, and non-repudiation of information. They must protect information systems from foreign and domestic attacks. They also must mitigate risk and conduct education and awareness programs.

CRITICAL INFRASTRUCTURE PROTECTION - ENDS, WAYS AND MEANS

The objective (end) of PDD 63 was to outline a presidential strategy to take the "...necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, especially our cyber systems."[73]

The strategic concept (ways) to accomplish the end is; 1) Set a goal of a reliable, interconnected, and secure information system infrastructure by the year 2003, and significantly increased security for government systems by the year 2000 by: Immediately establishing a national center to warn of and respond to attacks; Build the capability to protect critical infrastructures from intentional acts by 2003. 2) Address the cyber and physical infrastructure vulnerabilities of the Federal government by requiring each department and agency to work to reduce its exposure to new threats; 3) Requires the Federal government to serve as a model to the rest of the country for how infrastructure protection is to be attained; 4) Seeks the voluntary participation of private industry to meet common goals for protecting our critical systems through private-public partnerships; 5) Protects privacy rights and seeks to utilize market forces. It is meant to strengthen and protect the nations economic power, not to stifle it; 6) Seek full participation and input from the Congress.[74]

The resources (means) to the end are: 1) Appointed a national coordinator whose scope will include not only critical infrastructure but also foreign terrorism and threats of domestic mass destruction (including biological weapons) because attacks on the U.S. may not come labeled in neat jurisdictional boxes, 2) "Instituted the National Infrastructure Protection Center (NIPC) at the FBI which will fuse representatives from FBI, DoD, USSS, Energy, Transportation, the Intelligence Community and the private sector...,"[75] 3) An information Sharing and Analysis Center (ISAC) to be set up by the private sector in cooperation with the Federal government, 4) Create a National Infrastructure Assurance Council to draw from the private sector leaders and state/local officials to provide guidance to the policy formulation of a National Plan. 5) Create the Critical Infrastructure Assurance Office (CIAO) to provide support to the National Coordinator's work with government agencies and the private sector in developing a national plan.[76]

Has the Federal government developed the analysis, warning and information-sharing capabilities called for in PDD 63? Robert F. Dacey Director, Information Security Issues for the General Accounting Office (GAO) answered that question in testimony before the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, U.S. Senate in July of 2001. His answer - no, this has not been achieved.[77]

The reason for the failure is two-fold. First, to develop such a capability will take an intense interagency effort. Second, the Federal Bureau of Investigation's (FBI) National Infrastructure Protection Center's roles and responsibilities have not been clearly defined or uniformly interpreted by Federal agencies.[78] The bottom line is the NIPC strategy has not fully developed.

Has the Federal government formed a functioning interagency team that is protecting our critical infrastructure? According to a GAO report an interagency team has not been developed. The reason is the NIPC's inability to develop and synchronize an interagency process to deal with the information infrastructure coordinating challenges. As with many strategic issues interagency coordination has always been difficult in the Federal government.

Has the Federal Government developed a public/private partnership for critical infrastructure protection? The Federal government has not developed the robust public/private sector information sharing relationship that is necessary for critical infrastructure protection. There has been limited dialog with some private sector organizations such as the electrical power industry.

Has the NIPC developed the strategies necessary to mitigate risk to our critical infrastructure? According to a GAO report the NIPC has failed at that task. A key reason is because the FBI has failed to fill critical leadership positions at the NIPC. The report states "...the NIPC has sustained prolonged leadership vacancies and does not have adequate staff expertise, in part because other federal agencies have not provided the originally anticipated number of detailees."[79] From this comment in the GAO report it is evident that Federal agencies are not supporting the NIPC with the necessary manpower for success.

Is the United States better off after three years of PDD 63? I would argue, PDD 63 is not working well and we need to change our National Security Strategy to assure success.

RECOMMENDATIONS AND SOLUTIONS

The President must develop a solid, coherent and streamlined policy for critical infrastructure protection. I recommend the following changes to the critical infrastructure protection policy for America.

In the wake of the attack on America in September 2001, there must be strong and effective Presidential leadership, guidance, and direction for critical infrastructure protection.

There must be improved communication between federal agencies and the NIPC. With the right resources we can make government a model for information infrastructure protection. The President, through the Attorney General, FBI and NIPC should establish an interagency steering committee to develop roles and responsibilities of agency representatives to the NIPC.

The federal government should promulgate agency law that requires minimum technical specifications for critical infrastructures. Compliance with the agency law should be a prerequisite for contract award by the federal government. If a company were not in compliance with the minimum specifications it should affect bottom line or have a negative affect on shareholder wealth of publicly traded companies. Similarly state and local governments responsible for critical infrastructures that are subsidized by the federal government should meet minimum technical specifications in order to receive funding.

The National Coordinator for Information Assurance works for the Assistant to the President for National Security Affairs (see Table 2 above). The National Coordinator is responsible for the CIAO. This chain of responsibility is misplaced. The APNSA is responsible for advising the President and coordinating foreign policy, where as critical infrastructure protection is predominately an internal function of the federal government. The National Coordinator for Information Assurance and critical infrastructure protection should be placed under the newly formed Assistant to the President for Homeland Security.

Because of the uneasiness the private sector has with the NIPC being under the control of federal law enforcement, it should be moved away from the FBI. I recommend that the NIPC be placed under the control of the Assistant to the President for Homeland Security. This would separate law enforcement responsibilities of the FBI and information sharing duties of the NIPC.

The NIPC should study other interagency processes and model a successful program. There are other successful interagency programs that are working that can be exploited through lessons learned. We must also fund interagency liaison officers and agency cells at the NIPC to reinforce current NIPC manpower. The cells must be robust and filled with highly skilled and technical staffs. The President should mandate and enforce agency representation at the NIPC.

It order to have better coordination with the public sector the Federal government should provide funds to the ISAC communities to hire a representative to represent that ISAC at the NIPC. With ISAC representation at the NIPC, information could be pushed to member companies proactively. With ISAC representation at the NIPC there would be a closer public/ private partnership that would promote communication, coordination and cooperation.

Just like the NIPC should be moved from the control of the FBI, the InfraGard program should also be moved to another government agency also. I would recommend that InfraGard be moved to the Department of Commerce. Because the Department of Commerce is not a law enforcement arm of the federal government it would be better suited for educating the public and members on infrastructure protection and disseminating information through the InfraGard.

A weakness in protecting our critical infrastructure is the poor training and education programs for information technology professionals and their managers. In PDD 63, training and education is nearly absent. The Federal government must fund technical training and higher education for Federal, State and Local government employees that maintain critical infrastructure networks and associated computer systems. It should rapidly expand and fund the Cyber Corps training program.[80] Through the use of grants, scholarships and internships, managers at the NIPC and Federal agencies can invest in employees and employee training. They must also attract bright and intelligent people that want to serve in government, maintain information technology, and understand the interagency process.

Word Count = 7600

ENDNOTES

[1] William J. Clinton, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (Washington, D.C.: The White House, 22 May 1998), 4.

[2] U.S. House of Representatives, "Cyber Security - How Can We Protect American Computer Networks from Attack?" available from <http://www.house.gov/science/full/oct10/full_charter_101001.htm>; Internet; accessed 1 December 2001.

[3] George Smith, "The Moonlight Maze of Secret Cyberwar Gossip," 1999; available from <http://www.soci.niu.edu/~crypt/other/mmaze.htm>; Internet; accessed 1 December 2001.

[4] Ellen Messmer, "U.S.-China Hacker Brawl Draws Few Web Combatants," 5 July 2001; available from <http://www.nwfusion.com/archive/2001/120414_05-07-2001.html>; Internet; accessed 1 December 2001.

[5] Kevin Poulsen, "California Indicts Russian Hacker," 22 June 2001; available from <http://www.theregister.co.uk/content/8/19921.html>; Internet; accessed 1 December 2001.

[6] Smith.

[7] Floyd Norris, "Exchanges in New York Never Opened for the Day," 12 September 2001; available from <http://college3.nytimes.com/guests/articles/2001/09/12/867490.xml>; Internet; accessed 1 December 2001.

[8] Mark Harrington, "Attacks Cripple Local TV, Telephone Services," 12 September 2001; available from <http://www.newsday.com/entertainment/tv/ny-bzcomm122362134sep12.story>; Internet; accessed 1 December 2001.

[9] Ibid.

[10] Michael Arndt, "BW Online - Airlines: What Kind of Rescue?" 1 October 2001; available from <http://www.businessweek.com/magazine/content/01_40/b3751709.htm>; Internet; accessed 1 December 2001.

[11] William J. Clinton, A National Security Strategy for a Global Age (Washington, D.C.: The White House, December 2000), 4.

[12] William J. Clinton, Executive Order 13010 - Critical Infrastructure Protection (Washington, D.C.: The White House, 17 July 1996), 3.

[13] George W. Bush, "Using 21st Century Technology to Defend the Homeland," available from <http://www.whitehouse.gov/homeland/21st-technology.html>; Internet; accessed 15 February 2002.

[14] George W. Bush, "President Delivers State of the Union Address," 29 January 2002; available from <http://www.whitehouse.gov/news/releases/2002/01/20020129-11.html>; Internet; accessed 15 February 2002.

[15] John S. Tritak, “Critical Infrastructure Protection: Who’s In Charge?” 4 October 2001; available from <http://www.senate.gov/~gov_affairs/100401tritak.htm>; Internet; accessed 1 December 2001.

[16] U.S. State Department, “Regional Stability,” February 1999; available from <http://www.state.gov/www/global/general_foreign_policy/99_stratplan_goals2.html>; Internet; accessed 1 December 2001.

[17] Condoleezza Rice, "Understanding Risk and U.S. Economic Security," 22 March 2001; available from <http://usembassy.state.gov/tokyo/wwwhse0057.html>; Internet; accessed 1 December 2001.

[18] Clinton, Presidential Decision Directive 63, 4.

[19] Ibid., 1.

[20] Ibid., 2.

[21] Ibid., 4.

[22] Ibid.

[23] Ibid.

[24] Ibid.

[25] Ibid.

[26] Ibid., 5.

[27] Ibid.

[28] Ibid.

[29] Ibid.

[30] Ibid.

[31] Ibid.

[32] Ibid.

[33] National Defense University, Information Resource Management College, “Introduction to Information Operations” available from <http://ndu.blackboard.com/courses/1/AII0202/content/_24283_1/_19513_1/page7.html>; Internet; accessed 15 February 2002.

[34] Clinton, Presidential Decision Directive 63, 10.

[35] Ibid.

[36] Ibid.

[37] Ibid.

[38] Frances Wentworth, "Critical Infrastructure Protection: Establishing an Information Sharing and Analysis Center (ISAC) Can Be Like Developing an Organizational Security Policy," 26 September 2000; available from <http://www.sans.org/infosecFAQ/infowar/CIP.htm>; Internet; accessed 1 December 2001.

[39] Ibid.

[40] Ibid.

[41] Ibid.

[42] Ibid.

[43] Federal Bureau of Investigation, "National Infrastructure Protection Center (NIPC) - About NIPC - Critical Infrastructure," available from <http://www.nipc.gov/about/about4.htm>; Internet; accessed 3 December 2001.

[44] Heritage Foundation, Defending the American Homeland. A Report of The Heritage Foundation Homeland Security Task Force (Washington, D.C.: Heritage Foundation, 2002), 19.

[45] William J. Clinton, Defending America's Cyberspace, National Plan for Information Systems Protection Version 1.0 (Washington, D.C.: The White House, 2000), 4.

[46] Federal Bureau of Investigation.

[47] Ibid.

[48] Heritage Foundation, 19.

[49] Federal Bureau of Investigation.

[50] Heritage Foundation, 19.

[51] Federal Bureau of Investigation, "Critical Infrastructure"

[52] Ibid.

[53] Ibid.

[54] Heritage Foundation, 19.

[55] Ibid., 2.

[56] George W. Bush, Executive Order 13231 of 18 October 2001, Critical Infrastructure Protection in an Information Age (Washington, D.C.: The White House, 18 October 2001), 2.

[57] The President's Commission on Critical Infrastructure Protection, Critical Foundations, Thinking Differently (Washington, D.C.: The White House, 2000), 5.

[58] Federal Bureau of Investigation, "National Infrastructure Protection Center (NIPC) - About NIPC - Welcome," available from <http://www.nipc.gov/about/about.htm>; Internet; accessed 3 December 2001.

[59] Ibid.

[60] Federal Bureau of Investigation, "National Infrastructure Protection Center (NIPC) - Information Sharing - Outreach," available from <http://www.nipc.gov/infosharing/ infosharing.htm>; Internet; accessed 3 December 2001.

[61] Infragard, "Welcome to Infragard," available from <http://www.infragard.net>; Internet; accessed 4 January 2002.

[62] Federal Bureau of Investigation, "FBI Press Room - Press Release - 2000 - The FBI and the National Infrastructure Protection Center Publicly Introduce the National InfraGard Program," available from <http://www.fbi.gov/pressrel/ pressrel01/infragard.htm>; accessed 4 January 2002.

[63] Heritage Foundation14.

[64] Ibid., 17.

[65] Ibid., 18.

[66] Ibid.

[67] U.S. House of Representatives.

[68] Heritage Foundation, 15.

[69] Ibid.

[70] Ibid.

[71] U.S. Army War College, Information Operations Primer - Fundamentals of Information Operations (Carlisle Barracks: U.S. Army War College, 2001), 50.

[72] Clinton, Presidential Decision Directive 63, 5.

[73] Ibid.

[74] Federal Bureau of Investigation, "PDD 63 Protecting America's Infrastructures," available from <http://www.usdoj.gov/criminal/cybercrime/factsh.htm>; Internet; accessed 25 September 2001.

[75] Clinton, Presidential Decision Directive 63, 10.

[76] Ibid.

[77] General Accounting Office, Critical Infrastructure Protection Significant Challenges in Developing Analysis, Warning, and Response Capabilities (Washington, D.C.: U.S. General Accounting Office, 26 September 2001), 1.

[78] Ibid.

[79] Ibid.

[80] University of Tulsa, "Center for Information Security," available from <http://cis.utulsa.edu/CyberCorps>; Internet; accessed 15 February 2002.

BIBLIOGRAPHY

Arndt, Michael. "BW Online - Airlines: What Kind of Rescue?" 1 October 2001. Available from <http://www.businessweek.com/magazine/content/01_40/b3751709.htm>. Internet. Accessed 1 December 2001.

Bush, George W. "President Delivers State of the Union Address." 29 January 2002. Available from <http://www.whitehouse.gov/news/releases/2002/01/20020129-11.html>. Internet. Accessed 15 February 2002.

_________. "Using 21st Century Technology to Defend the Homeland." Available from <http://www.whitehouse.gov/homeland/21st-technology.html>. Internet. Accessed 15 February 2002.

_________. Executive Order 13231 of 18 October 2001, Critical Infrastructure Protection in an Information Age. Washington, D.C.: The White House, 18 October 2001.

Clinton, William J. A National Security Strategy for a Global Age. Washington, D.C.: The White House, December 2000.

_________. Executive Order 13010 - Critical Infrastructure Protection. Washington, D.C.: The White House, 17 July 1996.

_________. The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. Washington, D.C.: The White House, 22 May 1998

Federal Bureau of Investigation. "PDD 63 Protecting America's Infrastructures." Available from <http://www.usdoj.gov/criminal/cybercrime/factsh.htm>. Internet. Accessed 25 September 2001.

_________. "National Infrastructure Protection Center (NIPC) - About NIPC - Critical Infrastructure." Available from <http://www.nipc.gov/about/about4.htm>. Internet. Accessed 3 December 2001.

Harrington, Mark. "Attacks Cripple Local TV, Telephone Services." 12 September 2001. Available from <http://www.newsday.com/entertainment/tv/ny-bzcomm122362134sep12.story>. Internet. Accessed 1 December 2001.

Heritage Foundation. Defending the American Homeland - A Report of The Heritage Foundation Homeland Security Task Force. Washington, D.C.: Heritage Foundation, 2002.

Infragard. "Welcome to Infragard." Available from <http://www.infragard.net>. Internet. Accessed 4 January 2002.

Messmer, Ellen. "U.S.-China Hacker Brawl Draws Few Web Combatants." 5 July 2001. Available from <http://www.nwfusion.com/archive/2001/120414_05-07-2001.html>. Internet. Accessed 1 December 2001.

Norris, Floyd. "Exchanges in New York Never Opened for the Day." 12 September 2001. Available from <http://college3.nytimes.com/guests/articles/2001/09/12/867490.xml>. Internet. Accessed 1 December 2001.

Poulsen, Kevin. "California Indicts Russian Hacker." 22 June 2001. Available from <http://www.theregister.co.uk/content/8/19921.html>. Internet. Accessed 1 December 2001.

Rice, Condoleezza. "Understanding Risk and U.S. Economic Security." 22 March 2001. Available from <http://usembassy.state.gov/tokyo/wwwhse0057.html>. Internet. Accessed 1 December 2001.

Smith, George. "The Moonlight Maze of Secret Cyberwar Gossip." 1999. Available from <http://www.soci.niu.edu/~crypt/other/mmaze.htm>. Internet. Accessed 1 December 2001.

Tritak, John S. "Critical Infrastructure Protection: Who's In Charge?" 4 October 2001. Available from <http://www.senate.gov/~gov_affairs/100401tritak.htm>. Internet. Accessed 1 December 2001.

U.S. Army War College. Information Operations Primer - Fundamentals of Information Operations. Carlisle Barracks: U.S. Army War College, 2001.

U.S. General Accounting Office. Critical Infrastructure Protection Significant Challenges in Developing Analysis, Warning, and Response Capabilities. Washington, D.C.: U.S. General Accounting Office, April 2001.

U.S. House of Representatives. "Cyber Security - How Can We Protect American Computer Networks from Attack?" Available from <http://www.house.gov/science/full/oct10/full_charter_101001.htm>. Internet. Accessed 1 December 2001.

U.S. State Department. "Regional Stability." February 1999. Available from <http://www.state.gov/www/global/general_foreign_policy/99_stratplan_goals2.html>. Internet. Accessed 1 December 2001.

Wentworth, Frances. "Critical Infrastructure Protection: Establishing an Information Sharing and Analysis Center (ISAC) Can Be Like Developing an Organizational Security Policy." 26 September 2000. Available from <http://www.sans.org/infosecFAQ/infowar/CIP.htm>. Internet. Accessed 1 December 2001.